TÜV TRUST IT
TÜV AUSTRIA Group

Cyber Security

Technische Sicherheitsanalyse / Penetrationstest

Viele Unternehmen machen sich Gedanken über die Sicherheit ihrer IT, und das zu Recht. Denn die Angst vor finanziellen Schäden durch Hackerangriffe ist nicht unbegründet. Die Security-Analysts der TÜV TRUST IT finden die Schwachstellen Ihrer IT, können deren Risiken objektiv beurteilen und Ihnen dabei helfen, die Sicherheit zu steigern.

Vorgehensweise

Der beste Weg, um Ihre IT vor unberechtigten Angriffen zu schützen, ist die Durchführung regelmäßiger Penetrationstests. Die Penetrationstests der TÜV TRUST IT werden von unseren Experten mit langjähriger Praxiserfahrung durchgeführt. Zudem ist die TÜV TRUST IT vom Bundesamt für Sicherheit in der Informationstechnik (BSI) als IT-Sicherheitsdienstleister für die Geltungsbereiche Penetrationstest, IS-Revision und IS-Beratung zertifiziert.

Handeln wie ein „normaler“ Hacker

Unsere Prüfer orientieren sich bei ihrer Sicherheitsanalyse an der Vorgehensweise „normaler“ Hacker. Sie richten aber keinen Schaden an, sondern geben einen verständlichen Bericht ab, der Empfehlungen für sinnvolle Maßnahmen enthält.

Die Sicherheitsanalyse besteht aus fünf Phasen: Vorbereitung, Informationsbeschaffung, Bewertung, Eindringversuche und Erstellung des Berichts. In der ersten Phase wird geprüft, welche Bedrohungen es bei der zu untersuchenden Infrastruktur oder Applikation gibt. Mittels eines Bedrohungsmodells, einem sogenannten Threat-Model, wird unter anderem ermittelt, welche Sicherheitslücken durch das Zusammenwirken verschiedener Arbeitsbereiche entstehen, die für sich genommen vielleicht relativ sicher sind.

Unsere Security-Analysts gehen denselben Weg wie Hacker, die die „low-hanging fruits“ nutzen. Sie prüfen die Infrastruktur und suchen sich zum Angriff die schwächsten Punkte, um in das Netzwerk einzudringen. Sind sie erst einmal im Netzwerk, prüfen sie weitergehende Bedrohungen. Sie sammeln Informationen über die Netzwerkkomponenten, über Systeme, Dienste und Applikationen innerhalb des Untersuchungsbereichs. Dann versuchen sie Schwachstellen ausfindig zu machen und auszunutzen. So prüfen sie, ob sie sich als andere Benutzer ausgeben können (Spoofing Identity) oder Daten zu verändern (Tampering). Wichtig ist die Frage, ob Spuren verwischt werden können, indem beispielsweise das Logging umgangen wird. Zugriffe oder Änderungen können so keinem Nutzer zugeordnet werden (Repudation).

Fehlermeldungen sind eigentlich dafür gedacht, dem versierten Programmierer eine Hilfestellung zu geben. Sie können aber auch wertvolle Hinweise über das System enthalten, die von Angreifern missbraucht werden können. Dieses unerwünschte Durchsickern von Informationen nennt man Information Disclosure. Relativ bekannt sind Störungen von Diensten, die durch massive Zugriffe entstehen können. Das kann bis zu einem Denial of Service führen, durch den beispielsweise Ihre Website nicht mehr erreichbar ist. Durch solche Attacken können aber auch andere Dienste komplett blockiert oder Benutzerkonten gesperrt werden. Damit keine

Phasen der Sicherheitsanalyse

TÜV TRUST IT
TÜV AUSTRIA Group

Cyber Security

Systeme im Produktionsbetrieb gefährdet werden, führen wir solche Angriffe nur nach gesonderter Vereinbarung durch. Der letzte Test umfasst den Versuch, unbefugte Berechtigungen zu erlangen (Elevation of Privileges). Sollte dieser Erfolg haben, ist die Gefahr, dass sensible Daten in die falschen Hände gelangen, besonders groß. Diese Analyse erfolgt strukturiert nach anerkannten Standards wie der ISO/IEC 27001:2013 und nach Best Practice Ansätzen der TÜV TRUST IT. So bleiben Tests vergleichbar, wenn sie beispielsweise nach einem Jahr wiederholt werden.

Bundesamt für Sicherheit in der Informationstechnik
Zertifizierter IT-Sicherheitsdienstleister
Zertifikat Nummer: BSI-APS-9041
gültig bis 28.02.2025

Detaillierter Bericht mit Maßnahmenvorschlägen

Alle Ergebnisse der Untersuchung inklusive unserer Maßnahmenempfehlungen werden in einem verständlichen Abschlussbericht zusammengefasst. Unsere Security-Analysts bewerten und klassifizieren bereits während der Analyse die einzelnen Risiken. Wie wichtig die baldige Umsetzung ist, richtet sich nach der Klasse des Risikos. Wird eine unmittelbare Bedrohung der IT-Sicherheit festgestellt, wird der Kunde sofort informiert, um schnellstmöglich konkrete Gegenmaßnahmen einleiten zu können. In einem Abschlussworkshop wird der Bericht inklusive Management Summary präsentiert. Hier können dann sinnvolle und angemessene Maßnahmen zur Behebung der Schwachstellen diskutiert werden.

Ihr Nutzen

- Identifizierung von Schwachstellen in Ihrer IT und objektive Risikobeurteilung
- Abschlussbericht mit bewerteten und klassifizierten Risiken inklusive Empfehlung für entsprechende Verbesserungsmaßnahmen
- Vermittlung des umfangreichen Know-hows der neutralen und objektiven Auditoren der TÜV TRUST IT
- Die Kompetenzen der TÜV TRUST IT zur Durchführung von Penetrationstests wurden durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit der Zertifizierung zum zertifizierten IT-Sicherheitsdienstleister bestätigt.
- Erfüllung der Konformität zu Normen, u.a.:
  - DORA (Digital Operational Resilience Act)
  - TR-03109-6 Smart Meter Gateway Administration
  - ISO27001
  - IEC62443
  - Common Criteria

TÜV TRUST IT GmbH
Unternehmensgruppe TÜV AUSTRIA

Waltherstraße 49–51
D-51069 Köln
Tel.: +49 (0)221 969789 - 0
Fax: +49 (0)221 969789 -12

TÜV TRUST IT
TÜV AUSTRIA GmbH

TÜV AUSTRIA-Platz 1
2345 Brunn am Gebirge
Tel.: +43 (0) 5 0454 - 1000
Fax: +43 (0) 5 0454 - 76245

info@tuv-austria.com
www.it-tuv.com